CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS DE SEGURIDAD
AMENAZAS PERSISTENTES AVANZADAS (APT)

Una nueva clase de amenazas, conocidas como amenazas persistentes avanzadas (APT), ha atraído cada vez más la atención de los investigadores del sector de la Ciberseguridad. Las APT son ataques cibernéticos ejecutados por adversarios sofisticados y con una gran cantidad de recursos a disposición.
Están diseñadas para robar datos y comprometer infraestructuras críticas, las ame

¿Qué es una Amenaza Persistente Avanzada?

Es un ataque cibernético prolongado y dirigido en el que un intruso obtiene acceso a una red y permanece sin ser detectado por un período indeterminado de tiempo.

Es realizado a través de distintas técnicas, tácticas y procedimientos como, por ejemplo: Webshells, software de comando y control, software de acceso remoto, malware, spam, phishing, etc.

Propiedades del ataque

- **AMENAZA:** Identifica el uso de amenazas digitales para materializar el o los ataques.
- **PERSISTENTE:** indica que la naturaleza encubierta de la amenaza hace intentos reiterados de establecer el acceso a sistemas e información sensible de la organización.
- **AVANZADA:** significa la capacidad de superar los sistemas de detección de intrusos y mantener un acceso constante a la red objetivo de manera segura.

CARACTERÍSTICAS

1. **Son muy organizados:** Involucran varias personas, tecnologías y técnicas.
2. **Son eficientes**: Varían técnicas, tácticas y procedimientos según objetivos, a veces ingeniería social, otras utilizaran RAT, exploits 0-day o spear phishing.
3. **Son tenaces:** invierten los recursos que sean necesarios para lograr el objetivo.
4. **Son dirigidos:** Se enfocan en organizaciones específicas, individuos, estados, naciones, etc.

CARACTERÍSTICAS

5. **Son persistentes:** No es un evento de ataque específico, sino de actividades sistemáticas que permitan mantener el acceso a los sistemas el mayor tiempo posible.
6. **Son evasivos:** Pueden fácilmente camuflarse con los productos de seguridad tradicionales.
7. **Son complejos:** Combinan distintos métodos de ataque dirigidos a distintas vulnerabilidades.
8. **Impacto:** El impacto de un APT es proporcional a la permanencia del atacante en la red. En promedio, una amenaza de este tipo está unos 150 días en su objetivo.

RECOMENDACIONES

IDENTIFICAR todos los activos tecnológicos que componen el alcance a defender

DESARROLLAR arquitecturas de redes y sistemas, que contemplen medidas de ciberseguridad avanzadas

IMPLEMENTAR una correcta estrategia de registro y monitoreo de *logs*

ESTABLECER un plan de comunicaciones que ayude a los usuarios a comprender las amenazas y cómo identificarlas

CARACTERÍSTICAS

MANTENER el entorno TI con evaluación de vulnerabilidades y gestión eficiente de parches

ELIMINAR privilegios administrativos locales de las cuentas en estaciones de trabajo de los usuarios y limitar su acceso a lo necesario

DESARROLLAR pruebas de penetración y ejercicios prácticos de simulación de ataques que emulan actores APT

GENERAR conciencia de estos riesgos en la organización para formar estrategias de defensa eficaces

Ministerio del Interior y Seguridad Pública
Gobierno de Chile
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática
Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl

Síguenos en nuestras redes sociales
Infórmate sobre nuestras actividades y escríbenos directamente